204 – Steganography – Level 2

Team Information	
Team Name:	Barely Legal
Results Email:	[redacted]
Examination Time Frame:	to 10/31/08

Instructions

Description: Examiners must develop and document a methodology used to determine from the provided password protected files located in the **204_Steganography_Level2_Challenge2008** folder. Of the three files provided, identify the file that contains hidden data and extract and decode the hidden data.

Report with the exact detailed explanation of your process (software or technique) used to examine and detect the information, and then to successfully extract the information.

Total Weighted Points: 50 Total Points for correctly identifying the file containing hidden data – 150 points for extracting and decoding the hidden data. Total 200 Points Available

1. **Answers** – Fill in the chart below with your findings. *As a Forensic Challenge, consider that your answers will have to have enough detail for the Findings and Methodology of your examination to satisfy questioning in a court of law.*
2. **Methodology** – Provide a meticulously detailed explanation of your process. Be sure to include a step action that our reviewers can follow to reproduce your work for authenticity including tools and techniques.

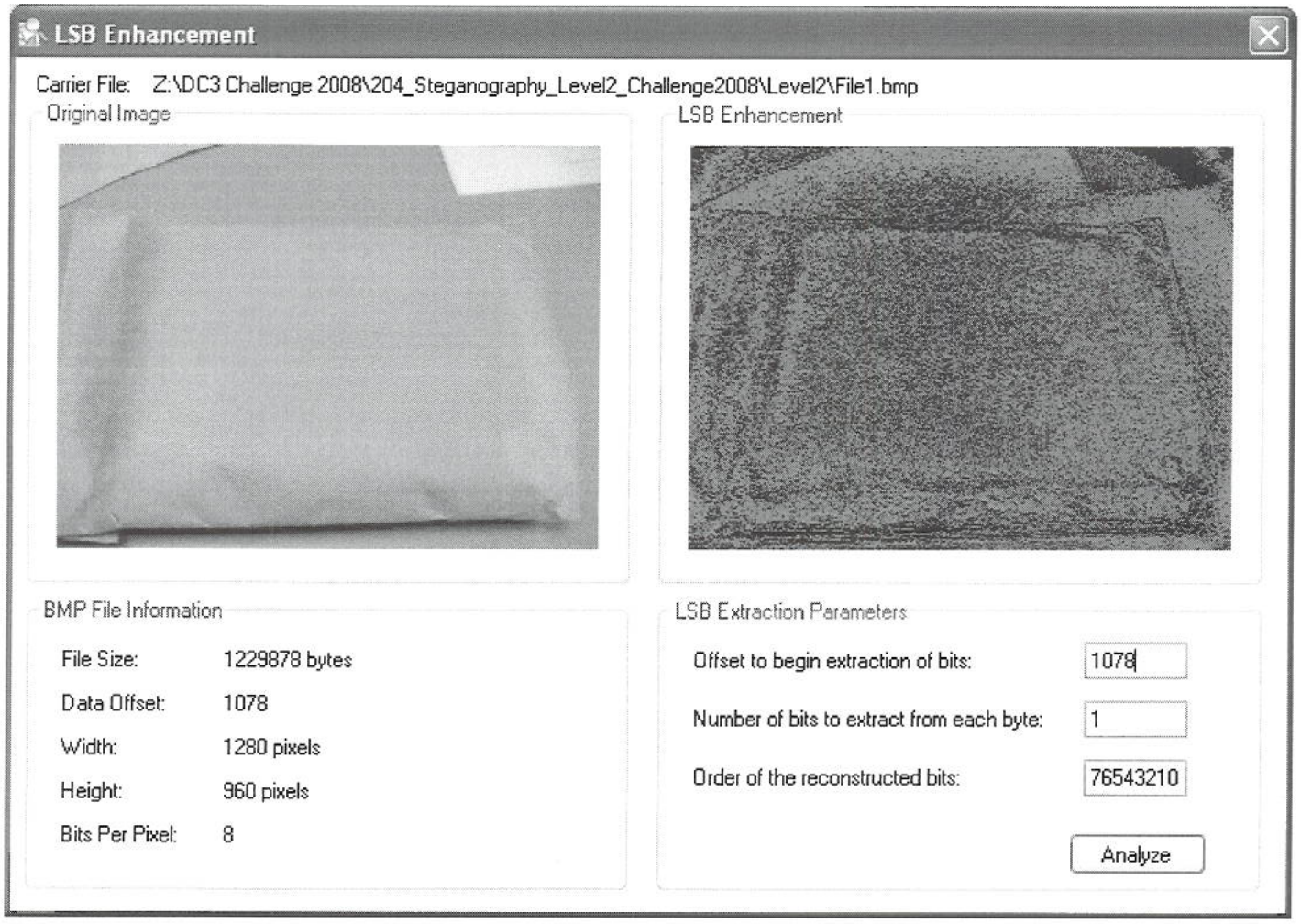
Internal Reviewer Use Only

Reviewer:		Points Awarded:	
Date:		Review Period:	to
Completed:	☐ Yes ☐ No ☐ Partial		

REPORT OF EXAMINATION

204 – Steganography Level 2

Of the three images provided, the "File1.bmp" image was identified as a file that may contain steganography imbedded using the Least Significant Bit technique.



The pattern of the extraction image is indicative of a secondary image (as opposed to ASCII text steganography), but the image could not be recovered in time.

METHODOLOGY / NOTES FORM

204 – Steganography Level 2

Date / Time	Notes
31-Oct-08 12:30 pm	Tool(s) Used: StegSpy by spyHunter (www.spy-hunter.com) Stegalyzer SS (30-day trial) by Backbone Security (www.sarc-wv.com) Analyzed all three images files with StegSpy and Stegalyzer SS. Process revealed "file1.bmp" was the image with steganography. Additional analysis with the "LSB Enhancement" process of Stegalyzer was unable to produce the decoded message/image.